What is claimed is:

1. A method for controlling, and distributing information between a digital postage meter and a certifying station operated by a certifying authority CA for publishing information, so that a public key $Key_{DM}*P$ of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from said published information with assurance that said public key $Key_{DM}*P$ has been certified by said certifying authority CA, said method comprising the steps of:

a) defining and publishing a finite group [P] with a binary operation [+] and publishing a particular point P in said group;

b) defining and publishing a binary operation K*P, where K is an integer and P is a point in said group, such that K*P is a point in said group computed by applying said operation [+] to K copies of said point P, and computation of K from knowledge of the definition of said group [P], said point P, and K*P is hard;

c) controlling a certifying station to publish a certificate $CERT_{DM}$ for said digital postage meter, wherein;

$$CERT_{DM} = (r_{DM} + r_{CA})*P;$$ and wherein

r_{DM} is a random integer generated by said digital postage meter and r_{CA} is a random integer generated by said certifying station;

d) controlling said certifying station to publish a message M;

e) controlling said certifying station to generate an integer I_{DM}, and send said integer to said digital postage meter, wherein;

$$I_{DM} = r_{CA} + H(M)Key_{CA};$$ and wherein

H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA;

f) publishing a public key $Key_{CA}*P$ for said certifying authority CA; and

g) controlling said digital postage meter to compute a private key Key_{DM},

$$Key_{DM} = r_{DM} + I_{DM} = r_{DM} + r_{CA} + H(M)Key_{CA;}$$ and

h) controlling said digital postage meter to print an indicium and digitally sign said indicium with said key Key_{DM}; whereby

i) said verifying party can compute said user's public key $Key_{DM}*P$ as

$$Key_{DM}*P = CERT_{DM} + H(M)\ Key_{CA}*P =$$

$$(r_{DM} + r_{CA})*P + H(M)Key_{CA}*P$$

from knowledge of H, M, [P], said public key $Key_{CA}*P$, and $CERT_{DM}$.

2. A method as described in claim 1 wherein said publicly known manner for deriving an integer from said published information comprises applying a hashing function to said message M.

3. A method as described in claim 2 wherein said message M includes information IAV identifying said digital postage meter and operating parameters applicable to said digital postage meter.

4. A method as described in claim 2 wherein said message M includes information IAV identifying said digital postage meter and operating parameters applicable to said digital postage meter.

5. A method as described in claim 1 wherein said group [P] is defined on an elliptic curve.

6. A method as described in claim 1 wherein said message M includes information tying said user's public key Key_U*P to said information IAV.

7. A article having an indicium imprinted thereon as evidence of attributes of said article, said indicium comprising:

a) a signature generated with a private key of a first party;

b) a certificate;

c) information specifying attributes of said article; wherein

d) said private key of said first party is generated as a function of said certificate, said information, and a private key of a certifying authority, said function being chosen so that a party wishing to verify said indicium can determine a public key corresponding to said private key of said first party by operating on said certificate and said information with a corresponding public key of said certifying authority.

8. A method for controlling a digital postage meter to print indicia signed with a private key Key_{DM} based upon a published a finite group [P] with a binary operation [+] and a published particular point P in said group and a published a binary operation K*P, where K is an integer and P is a point in said group, such that K*P is a point in said group computed by applying said operation [+] to K copies of said point P, and computation of K from knowledge of the definition of said group [P], said point P,

d) said first function, said second function and said published related information are chosen so that a party seeking to verify said indicia can compute said digital postage meter public key by operating on said published related information with said published public key of said authority.

11. A method as described in claim 10 wherein said published related information includes information identifying said digital postage meter and operating parameters applicable to said digital postage meter.

12. A method for certification by a certifying authority of a public key of a digital postage meter, said digital postage meter producing indicia signed with a corresponding private key of said digital postage meter, said certifying authority having a published public key and a corresponding private key, said method comprising the steps of:

a) said certifying authority providing a user with an integer, said integer being a first function of said private key of said authority;

b) said user computing a digital postage meter private key as a second function of said integer and downloading said postage meter private key to said digital postage meter; and

c) said certifying authority publishing related information; wherein

d) said first function, said second function and said published related information are chosen so that a party seeking to verify said indicia can compute said digital postage meter public key by operating on said published related information with said published public key of said authority.

5 ~~13~~. A method as described in claim 4 ~~12~~ wherein said published related information includes information identifying said digital postage meter and operating parameters applicable to said digital postage meter.

add a3

add a5

add a6

ADD B7

ADD B9

and K*P is hard, so that a public key Key_{DM}*P of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from published information with assurance that said public key Key_{DM}*P has been certified by a certifying authority CA, said method comprising the steps of:

a) controlling said digital postage meter to generate a random number r_{DM} and send a point r_{DM}*P to a certifying station;

b) controlling said digital postage meter to receive a certificate $CERT_{DM}$ from a certifying station operated by said certifying authority CA, wherein;

$$CERT_{DM} = (r_{DM} + r_{CA})*P; \text{ and wherein}$$

r_{DM} is a random integer generated by said digital postage meter and r_{CA} is a random integer generated by said certifying station;

c) controlling said digital postage meter to receive an integer I_{DM} from said certifying station, wherein;

$$I_{DM} = r_{CA} + H(M)Key_{CA;} \text{ and wherein}$$

M is a message published by said certifying station and H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA;

d) controlling said digital postage meter to compute a private key Key_{DM},

$$Key_{DM} = r_{DM} + I_{DM} = r_{DM} + r_{CA} + H(M)Key_{CA;} \text{ and}$$

e) controlling said digital postage meter to print an indicium and digitally sign said indicium with said key Key_{DM}; whereby

f) said verifying party can compute said digital postage meter public key Key_{DM}*P as

$$Key_{DM}*P = CERT_{DM} + H(M)\ Key_{CA}*P =$$

$(r_{DM}+r_{CA})*P + H(M)Key_{CA}*P$

from knowledge of H, M, [P], said public key $Key_{CA}*P$, and $CERT_{DM}$.

9. A method for controlling a certifying station operated by a certifying authority CA to publish information relating to a digital postage meter for printing indicia signed with a private key Key_{DM} based upon a published a finite group [P] with a binary operation [+] and a published particular point P in said group and a published a binary operation K*P, where K is an integer and P is a point in said group, such that K*P is a point in said group computed by applying said operation [+] to K copies of said point P, and computation of K from knowledge of the definition of said group [P], said point P, and K*P is hard, so that a public key $Key_{DM}*P$ of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from said published information with assurance that said public key $Key_{DM}*P$ has been certified by a certifying authority CA, said method comprising the steps of:

a) controlling said certifying station to receive a point $r_{DM}*P$ from said digital postage meter, where r_{DM} is a random number generated by said digital postage meter;

b) controlling said certifying station to generate and send to said digital postage meter a certificate $CERT_{DM}$, wherein;

$CERT_{DM} = (r_{DM} + r_{CA})*P$; and wherein

r_{CA} is a random integer generated by said certifying station;

c) controlling said certifying station to generate and send to said digital postage meter an integer I_{DM}, wherein;

$I_{DM} = r_{CA} + H(M)Key_{CA;}$ and wherein

M is a message published by said certifying station and H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA; whereby

d) said digital postage meter can compute said private key Key_{DM},

$$Key_{DM} = r_{DM} + I_{DM} = r_{DM} + r_{CA} + H(M)Key_{CA};$$ and

and digitally sign said indicium with said key Key_{DM}; and whereby

e) said verifying party can compute said digital postage meter public key $Key_{DM}*P$ as

$$Key_{DM}*P = CERT_{DM} + H(M)\ Key_{CA}*P =$$

$$(r_{DM} + r_{CA})*P + H(M)Key_{CA}*P$$

from knowledge of H, M, [P], said public key $Key_{CA}*P$, and $CERT_{DM}$.

10. A method for certification by a certifying authority of a public key of a digital postage meter, said digital postage meter producing indicia signed with a corresponding private key of said digital postage meter, said certifying authority having a published public key and a corresponding private key, said method comprising the steps of:

a) said certifying authority providing said meter with an integer, said integer being a first function of said private key of said authority;

b) said meter computing a digital postage meter private key as a second function of said integer; and

c) said certifying authority publishing related information; wherein